DATA ENCRYPTION POLICY

The University of Arkansas at Pine Bluff is committed to a computing system, which effectively meets the needs of users. The University of Arkansas at Pine Bluff enhances teaching, research, service and activities, which support them, provides computing resources.

Individuals who are granted computing accounts or use computing resources at the University of Arkansas at Pine Bluff accept responsibility with such access. Each user is expected to use accounts or resources within the University approved educational, research, or administrative purposes for which they are granted. Activities beyond these stated purposes are strictly prohibited.

A Data Encryption Policy for the University is stated below. This document describes the overall policy and expectations related to the encryption of business important files which reside on client computing equipment. Violations of this policy will be reviewed through established University judicial and administrative procedures. Actions to restrict computer usage may be challenged through the same procedures.

These documents have been voluntarily contributed by NOREX members with the full knowledge that other members may use them in any manner they see fit. University of Arkansas Pine Bluff is a member of NOREX.

Introduction

This policy covers the encryption of sensitive data. Sensitive data is defined in this document to include some of the following (This is not an all-inclusive list)

- Personal Identifiable Information
    - ❖ First and Last Name or first initial and last name in combination with any of the following:
        - Social Security number
        - Driver's license number
        - Bank Account, Credit, or Debit card account number
        - UAPB password
- Private, confidential, or personal information
    - ❖ Name, Address, and Date of Birth
    - ❖ Records protected by HIPPA, FERPA, GLBA, or other applicable federal law or regulation

ENCRYPTION FOR TRANSMISSION OF SENSITIVE DATA

The purpose of this document is to describe the overall policy and expectations related to the data encryption of business important files.

1. **Backups** – All data being backed up needs to be encrypted
2. **Emails** – Transmitting emails with sensitive information needs to be encrypted with encryption software
3. **File transfers** – File transfers with sensitive data needs to be encrypted across the network using a secure protocol such as SFTP
4. **Network Device Access** - Remote access logins to network devices needs to be encrypted with a secure protocol such as SSH (Secure Shell)
5. **Passwords** – Passwords should always be encrypted when transmitted across the network using secure protocols such as Microsoft Active Directory Kerberos, and SSH
6. **Sensitive data** – Sensitive data needs to be encrypted across the network when clients access web sites. Web sites and browsers need to use up to date SHA certificates and protocols such as SHA2 (2048 bits) certificates, https with TLS, (Hypertext Transfer Protocol Secure with Transport Layer) and up to date ciphers
7. **Server Remote Access** – Remote access logins to servers on the network needs to be encrypted with secure protocols such as SSH for Linux/AIX and RDP (Remote Desktop Protocol) with high TLS encryption for Windows
8. **VPN** – Accessing the campus network from off campus via the VPN (Virtual Private Network) needs to be encrypted using secure protocols such as SHA2 certificates, TLS 1.X protocols, and up to date ciphers on its VPN access

ENCRYPTION OF SENSITIVE DATA ON PORTABLE DEVICES

1. **Laptops, tablets, iPads, USB devices, etc.** – Sensitive data should not be installed on a portable device, because they have the potential to be lost or stolen. If there is a valid reason to store sensitive data, then the data needs to be encrypted at rest. Windows devices can be encrypted using Windows Bitlocker, and Apple Macs can be encrypted using Apple FileVault encryption. In addition, there are freeware and paid encryption programs that can be used for encryption.
2. Any drives sent outside the University for repair, that contain sensitive data must be either encrypted at rest (if possible), or the data removed (if possible)

Policy

This policy was documented by Willette Totten, Director of Information Technology Services, on October 1, 2019.

REFERENCES AND RELATED DOCUMENTS

Dept. of Homeland Security Handbook for Sensitive Personally Identifiable Information
Wikipedia on Personally Identifiable Information

Caution

Encrypting data makes it unreadable, unless the software managing the encryption algorithm is presented the appropriate credentials and keys to unlock the encrypted data. This means that if the appropriate authentication and/or keys are unavailable or become corrupted, data could be lost. ***Example:*** *a laptop has been configured to encrypt the entire hard drive – if the user forgets the password or cannot access the key(s), the data and the entire system will not be recoverable.* When transferring data from a device with encrypted data to another device, it must remain encrypted.

Technical Services strongly recommends storage on enterprise servers – not on single-user devices, such as workstations, laptops, mobile devices, smartphones, cell phones or external storage media.